ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mobilné siete

Univerzita Komenského, 2019

Mgr. Ján Kotrady

Kľúčové slová

- Ki
- Kc
- RAND
- SRES (XRES)
- RES
- A3, A5
- IMSI – 15 čísel
- AUTN, MAC, SQN

+421 2 59 278 262
jan.kotrady@csirt.sk

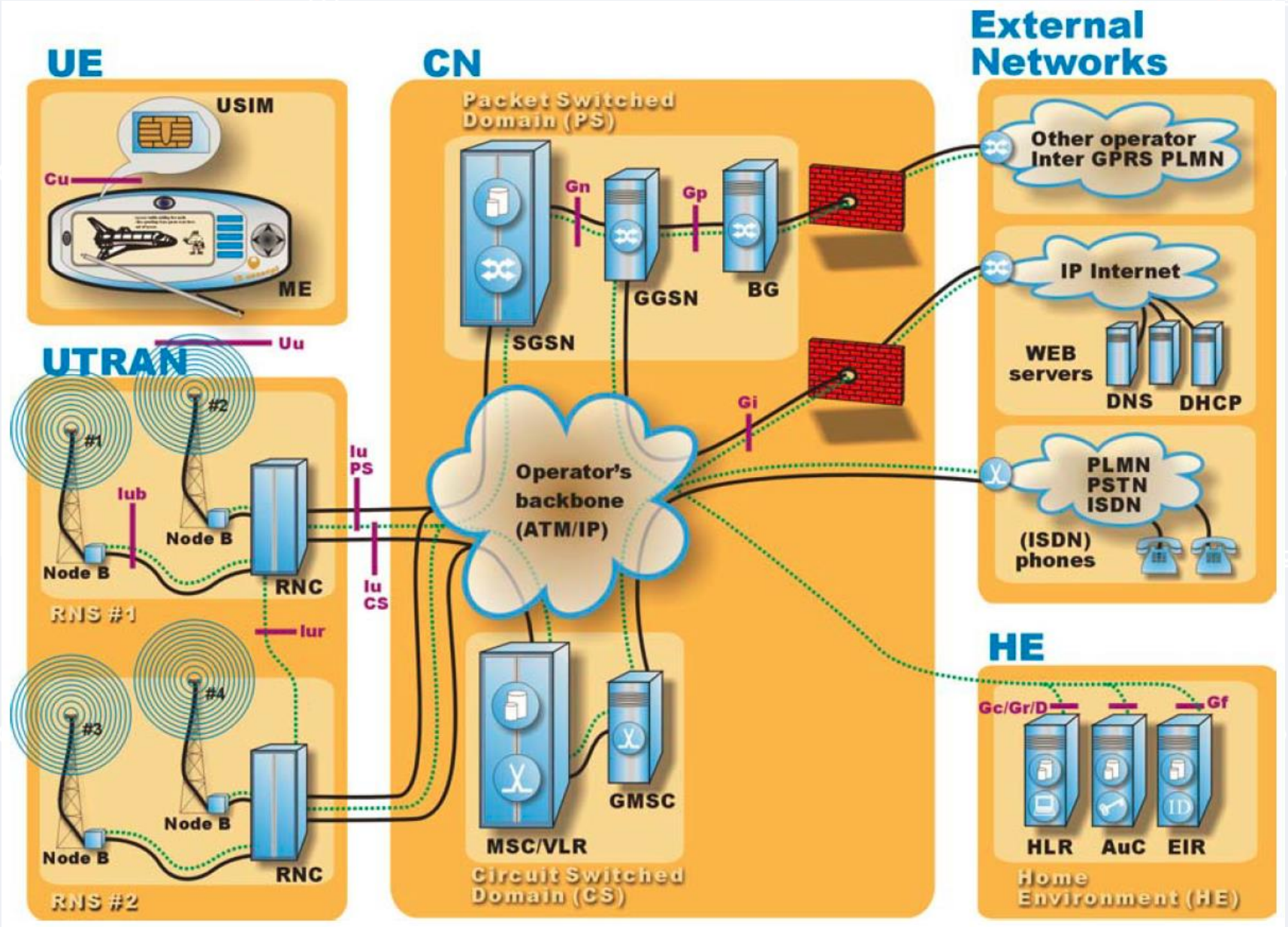
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Kľúčové slová

- USIM - Universal Subscriber Identity Module
- UE - User Equipment
- SRNC - Serving Radio Network Controller
- VLR - Visitor Location Register
- SQN - Sequence number
- AuC - Authentication Centre
- AUTN | S - Authentication token | Synchronization

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

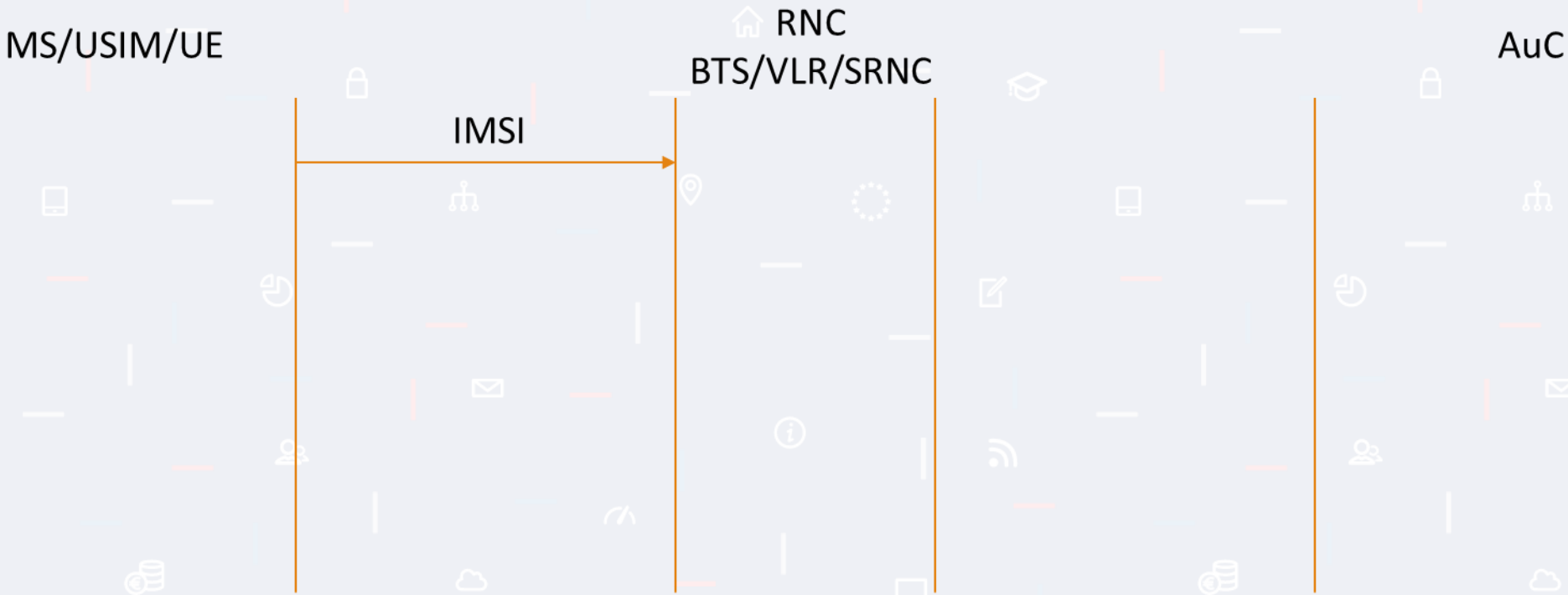

UE
USIM
Cu
ME
Uu
UTRAN
#1
#2
#3
#4
Node B
Node B
Node B
Node B
Iub
Iur
RNC
RNC
RNS #1
RNS #2
Iu PS
Iu CS
CN
Packet Switched Domain (PS)
SGSN
GGSN
BG
Gn
Gp
Gi
Operator's backbone (ATM/IP)
MSC/VLR
GMSC
Circuit Switched Domain (CS)
External Networks
Other operator Inter GPRS PLMN
IP Internet
WEB servers
DNS
DHCP
PLMN
PSTN
ISDN
(ISDN) phones
HE
Gc/Gr/D
Gf
HLR
AuC
EIR
Home Environment (HE)

GSM autentifikácia

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

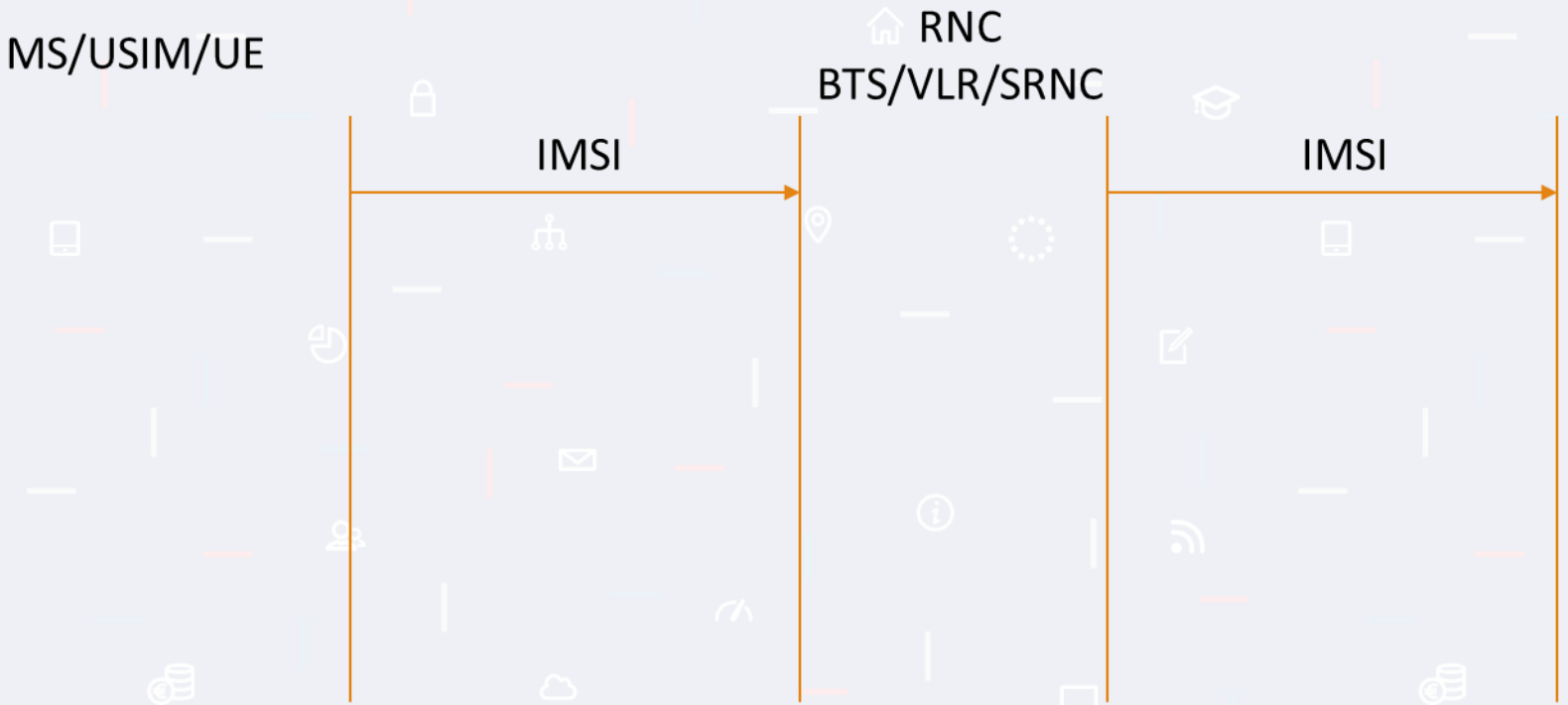
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

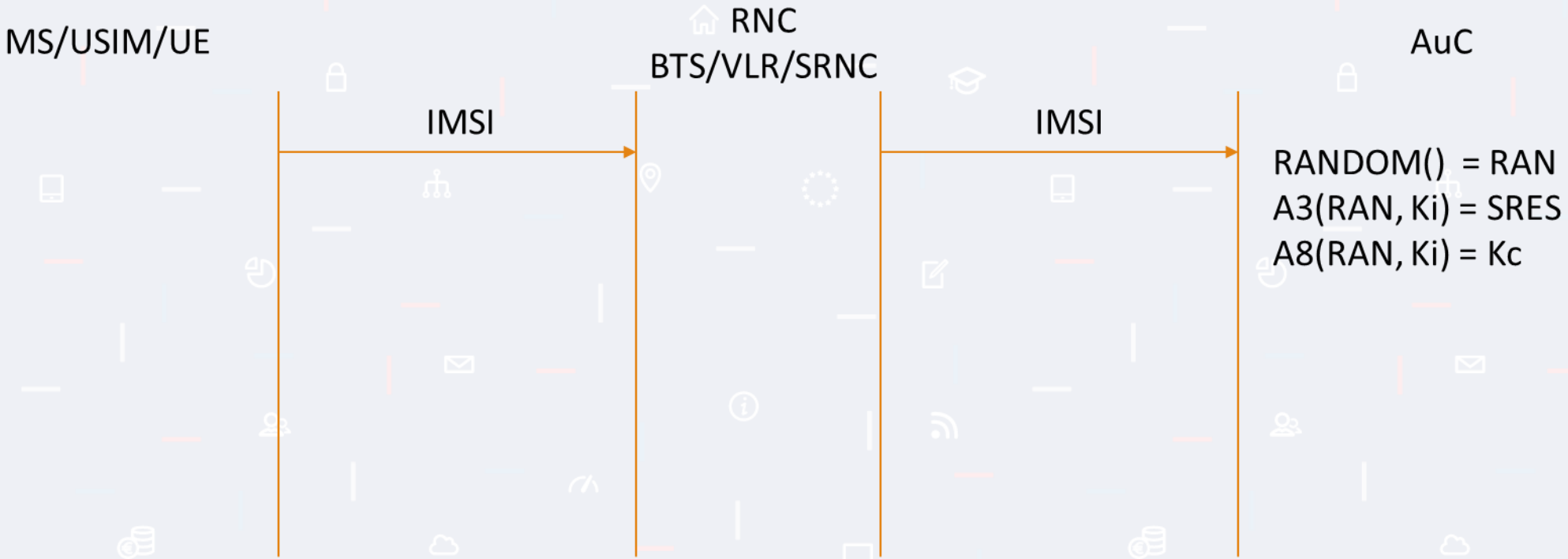
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

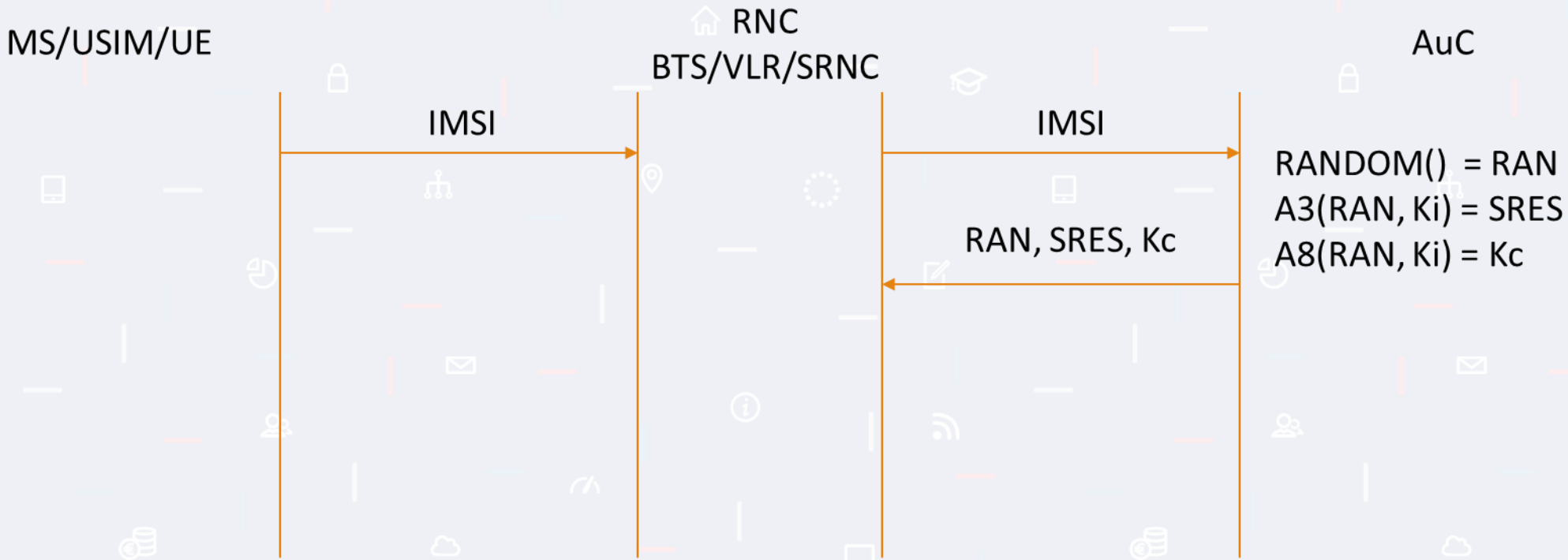
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

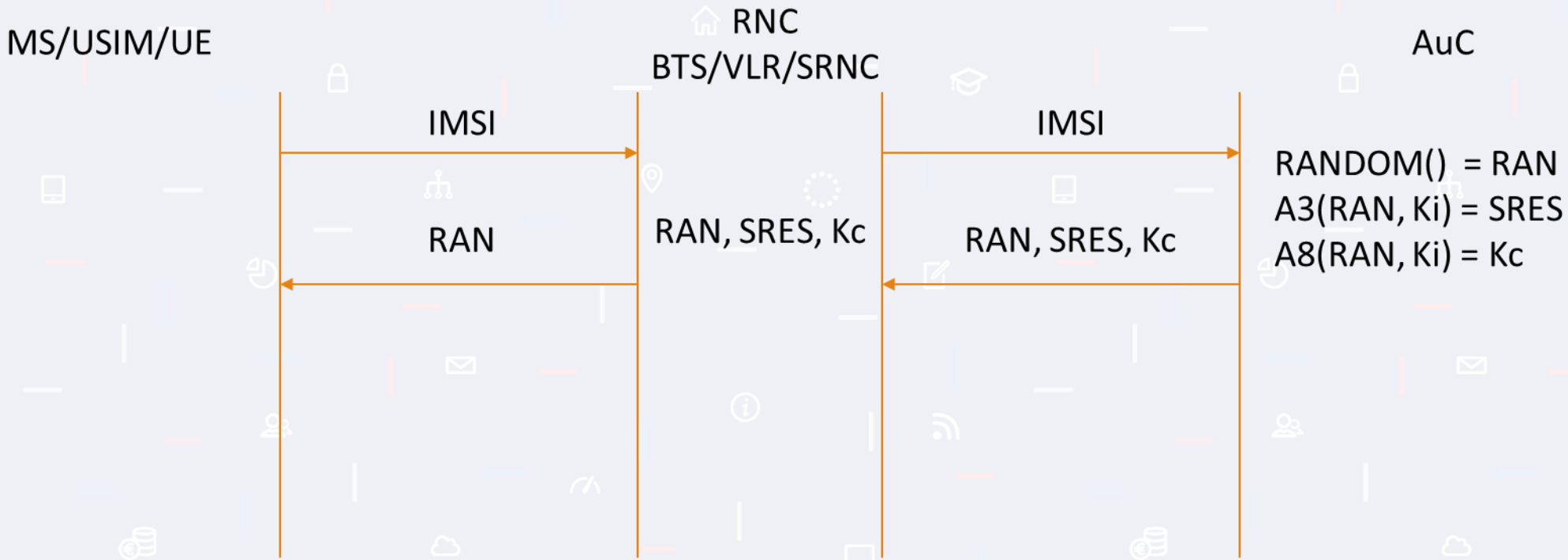
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

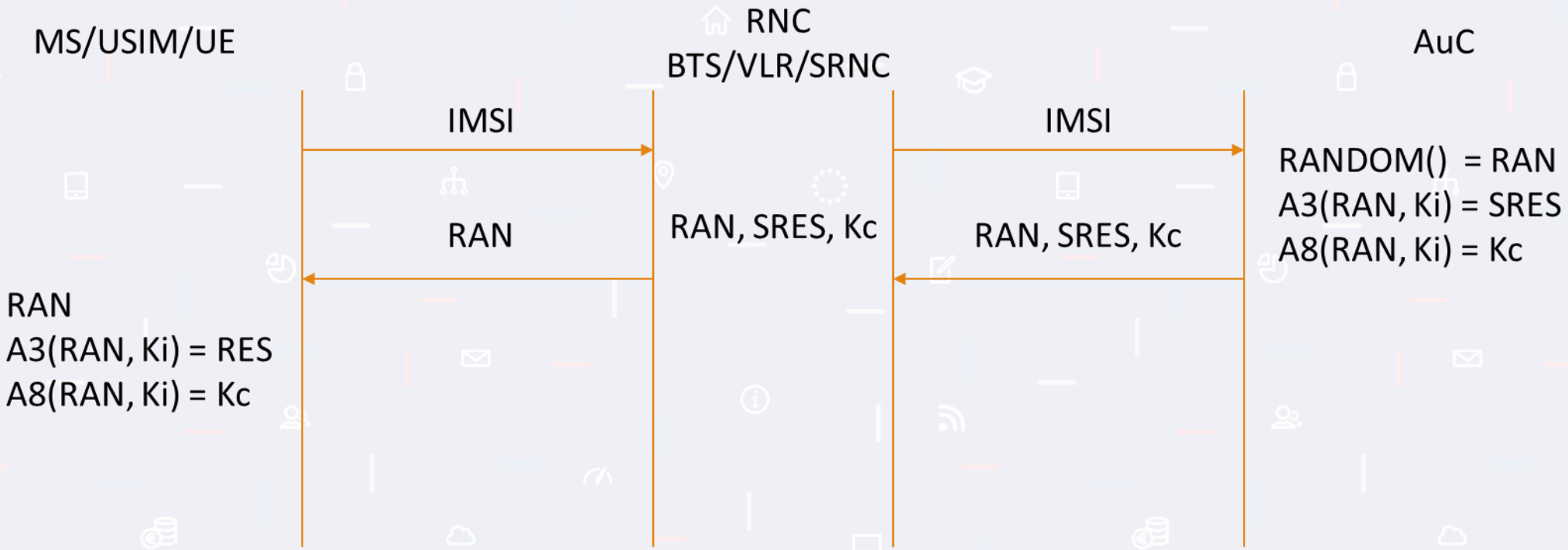
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

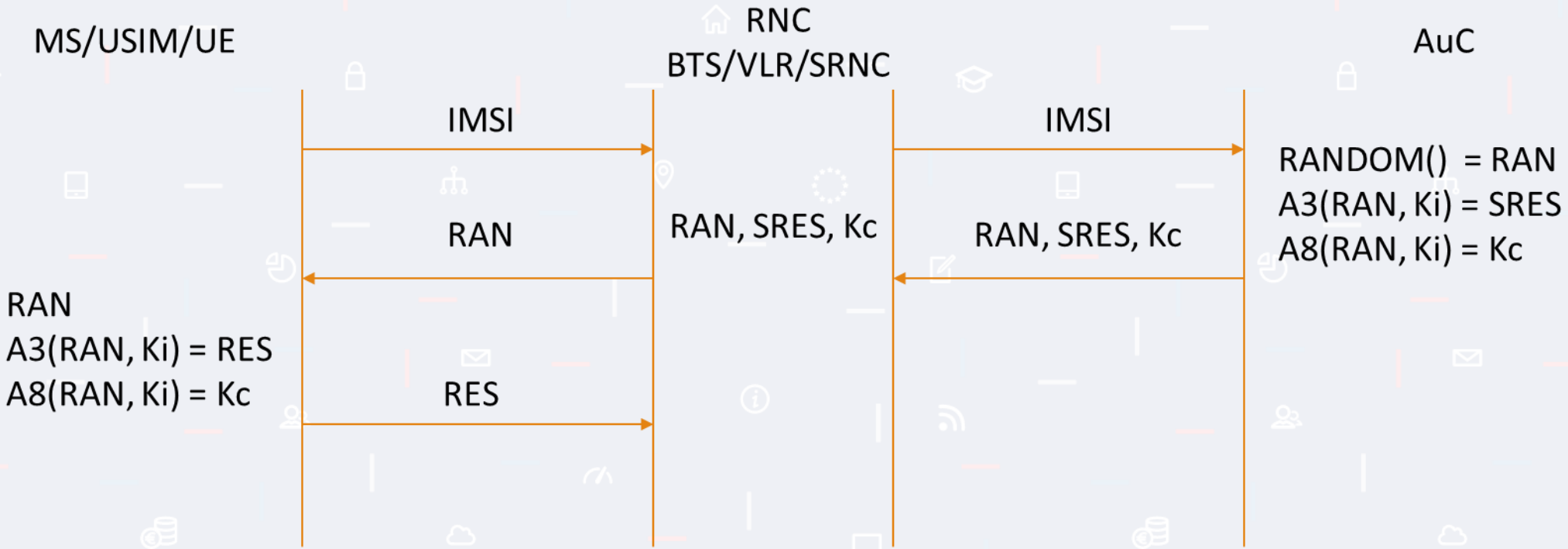
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

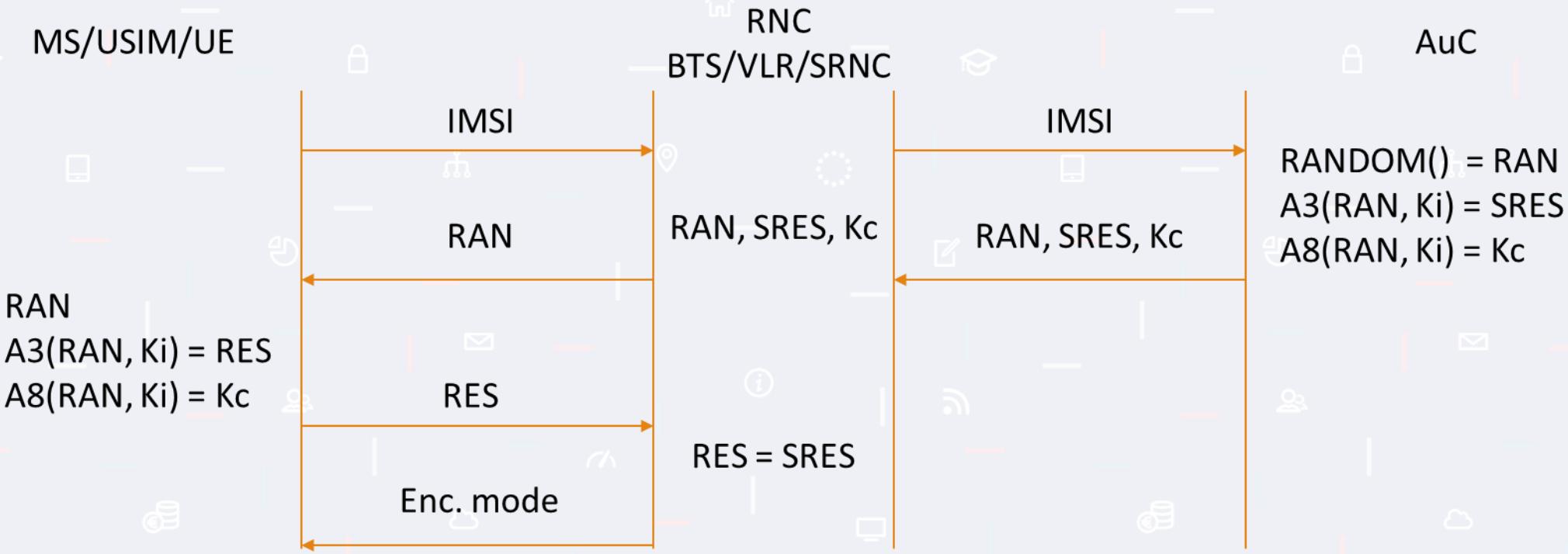
GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

GSM autentifikácia



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

História chýb algoritmov

- 1991 – GSM implementácia
- Apríl 1998 - The Smartcard Developer Association (SDA) spolu s U.C. Berkeley researches prelomili COMP128 algoritmus uložený v SIM karte a úspešne získali Ki v priebehu pár hodín. Zistili, že Kc používa iba 54 bitov.
- August 1999: Slabá A5/2 bola prelomená použitím PC v priebehu pár sekúnd.
- December 1999: Alex Biryukov, Adi Shamir a David Wagner publikovali schému útoku na algoritmus A5/1. Pri získaní dvoch minút rozhovoru boli schopný prelomiť A5/1 algoritmus v priebehu 1 sekundy.
- Máj 2002: IBM Research group objavila nový spôsob rýchleho získavania Kc z COMP128 použitím útokov side channels.

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE

Fukncia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	…	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na karte – zdieľaný	Žiadny	USIM, AuC		128

+421 2 59 278 262
jan.kotrady@csirt.sk

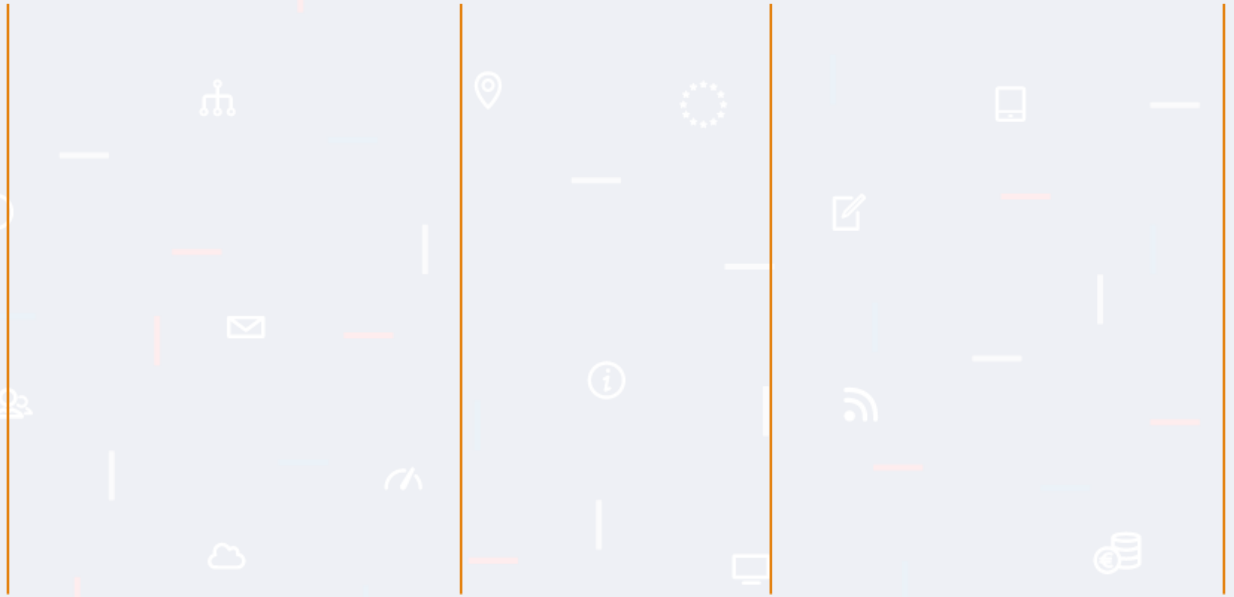
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

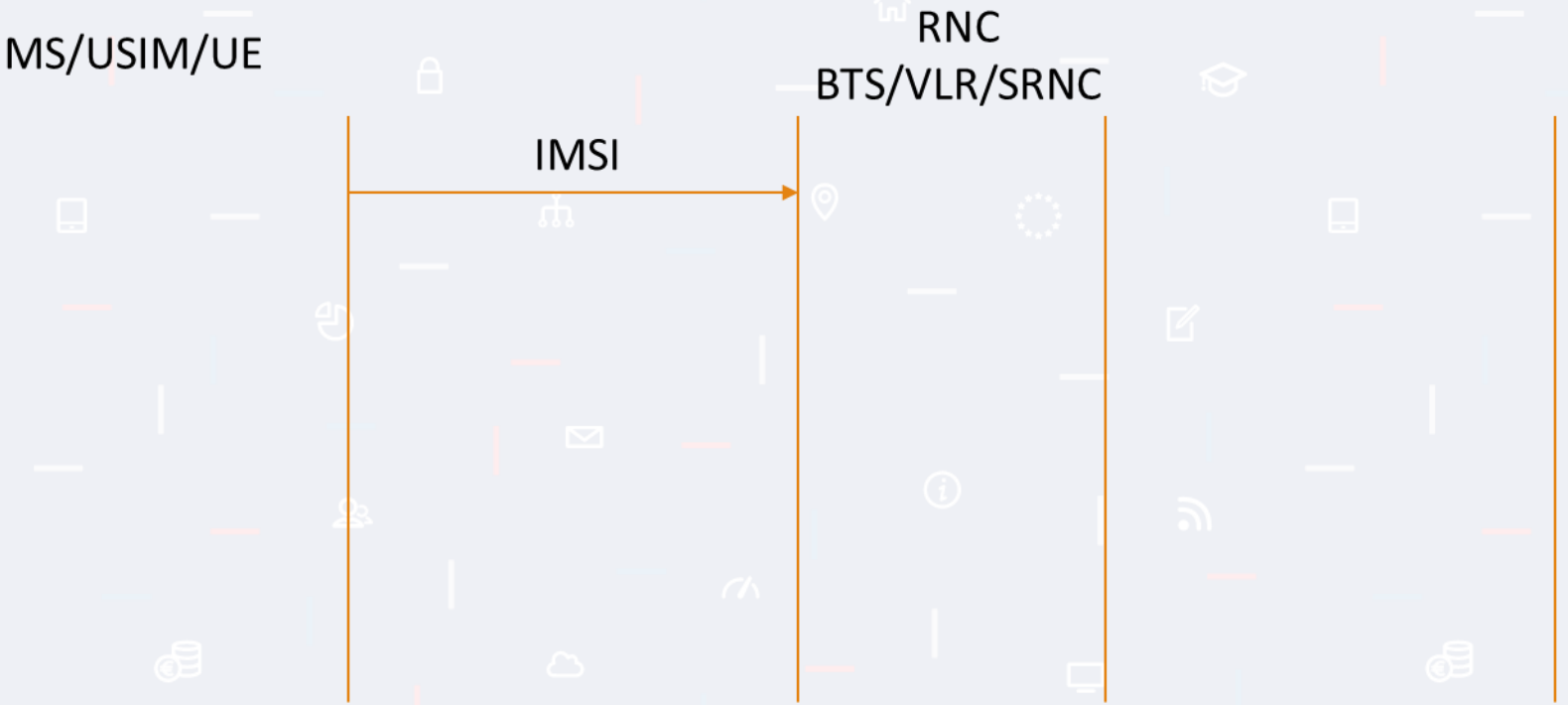
AuC



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

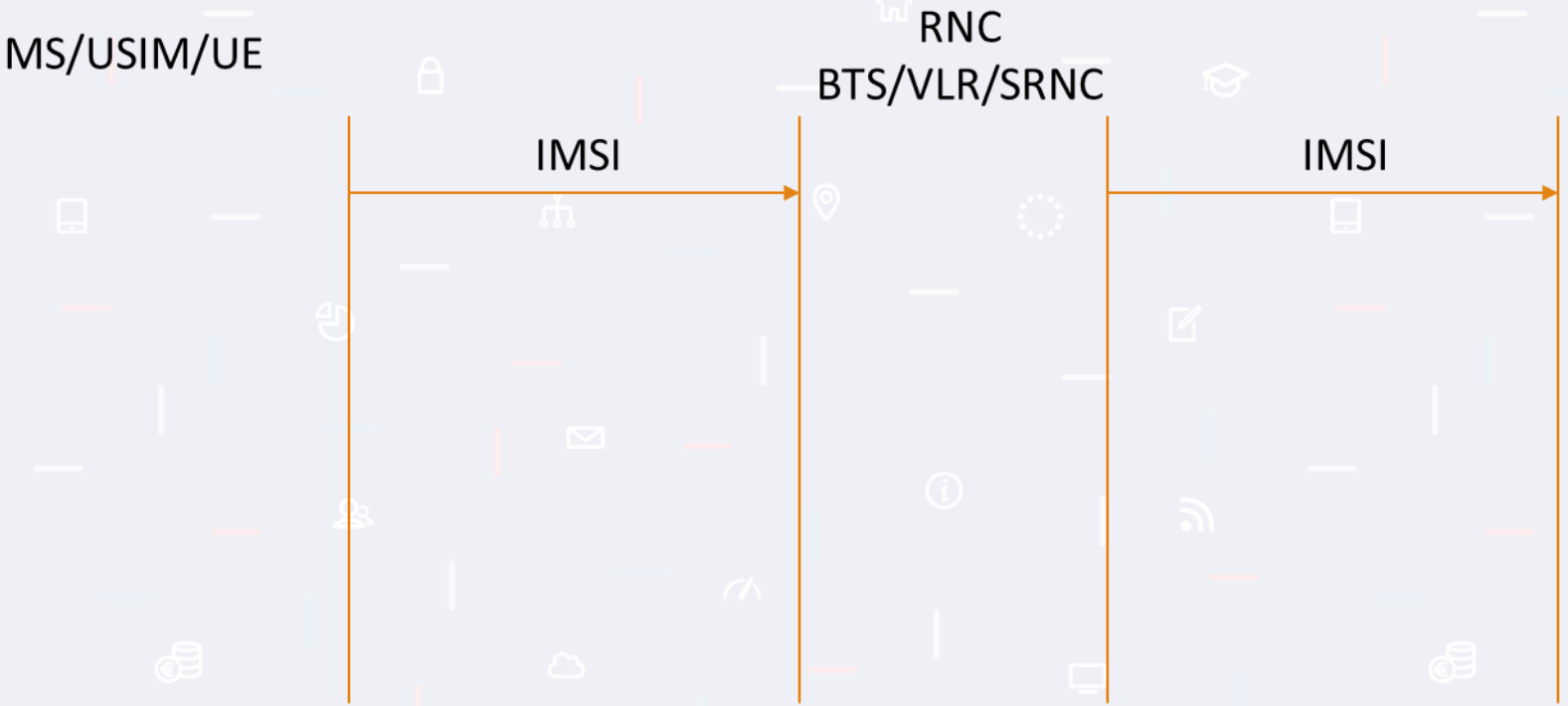
3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

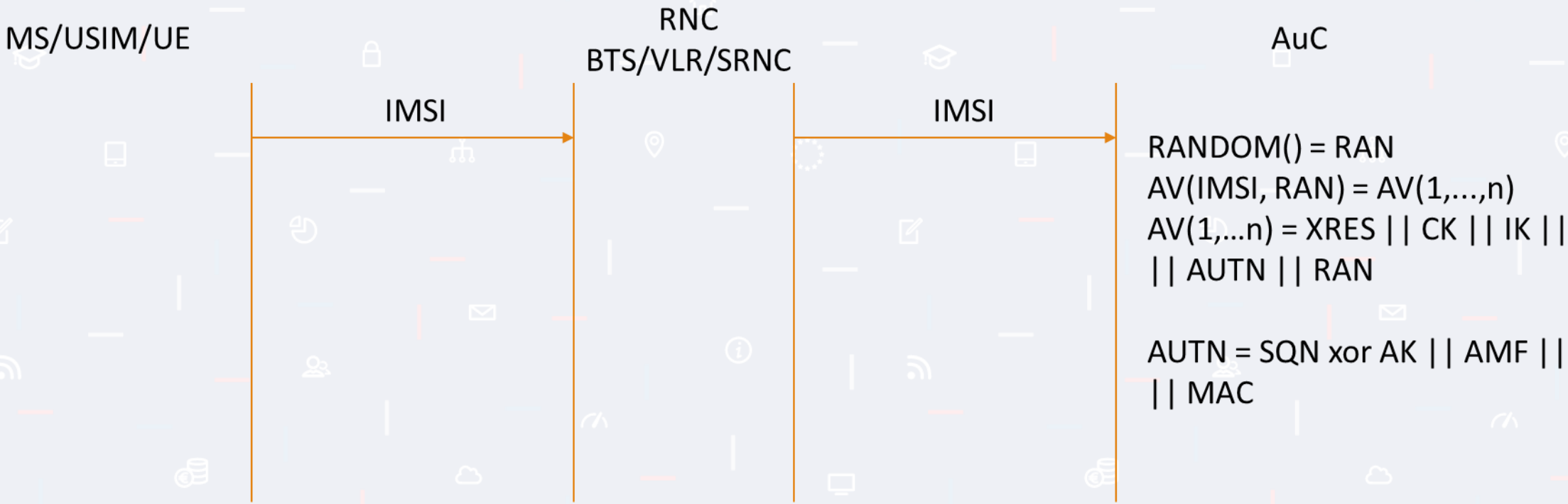
3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

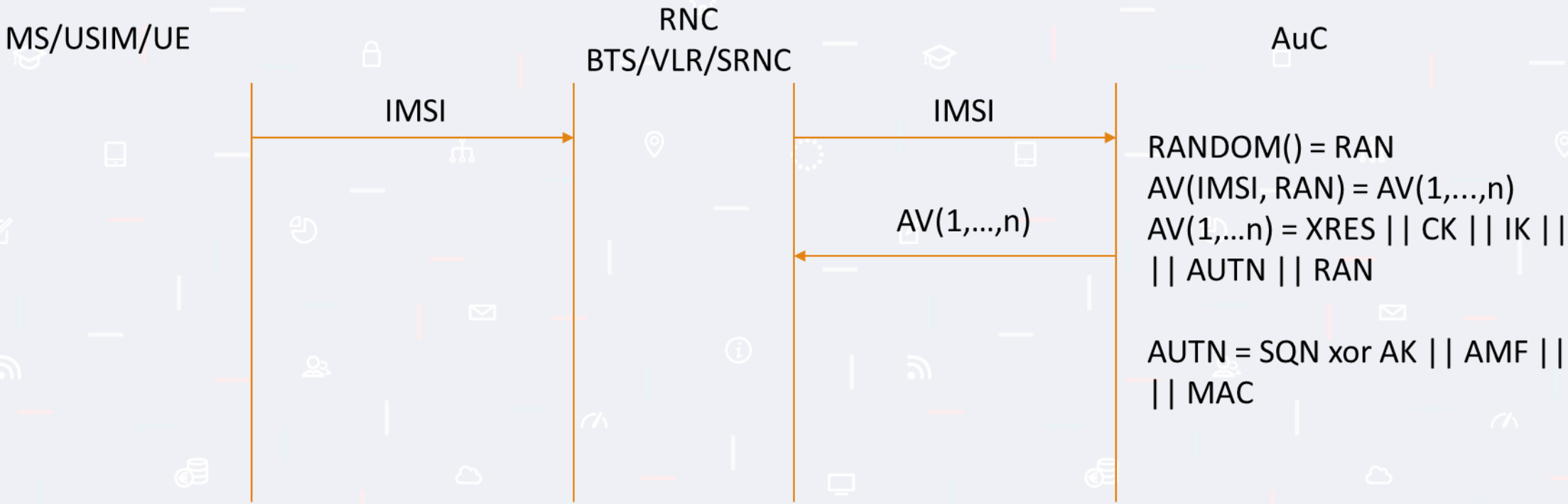
3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk

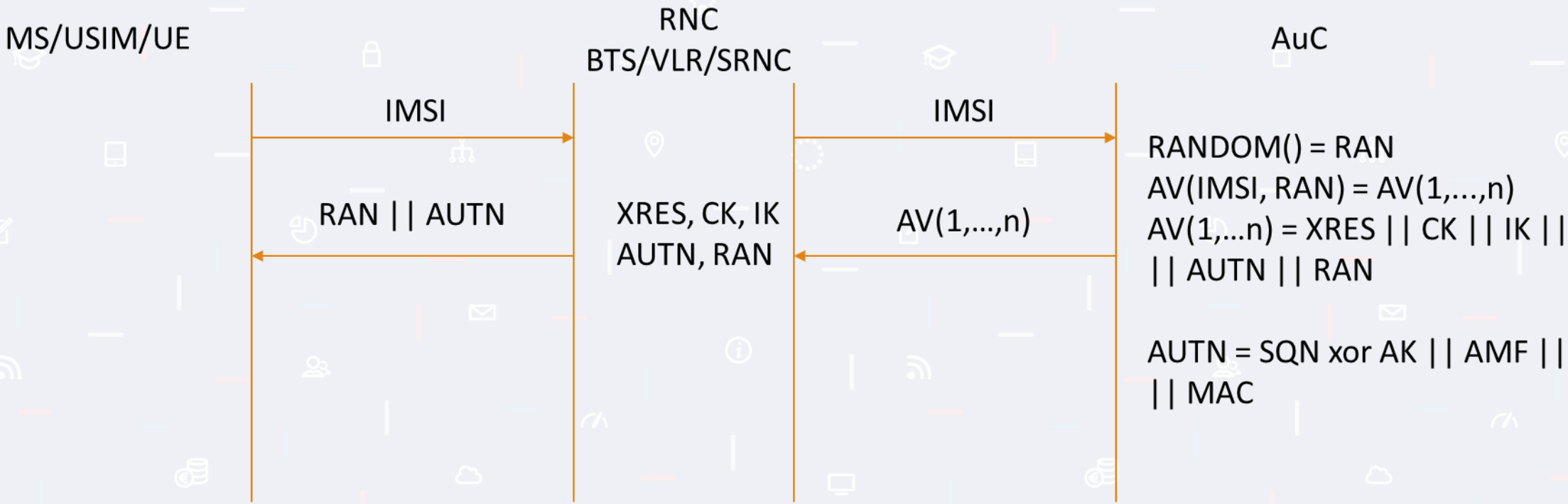
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE



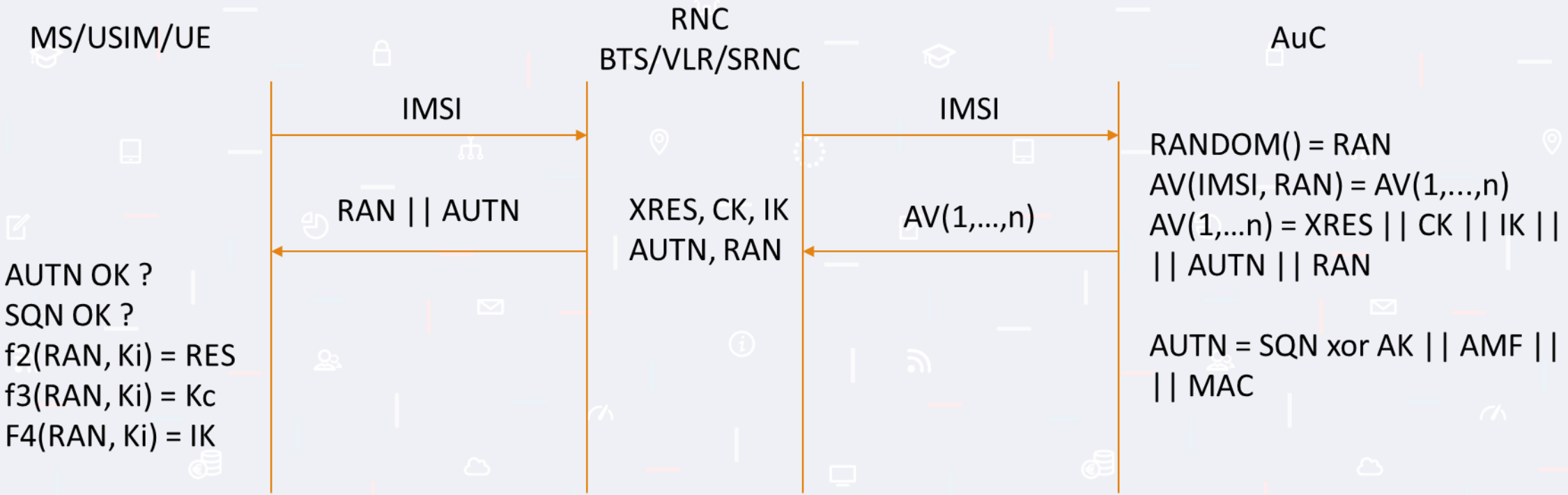
+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE



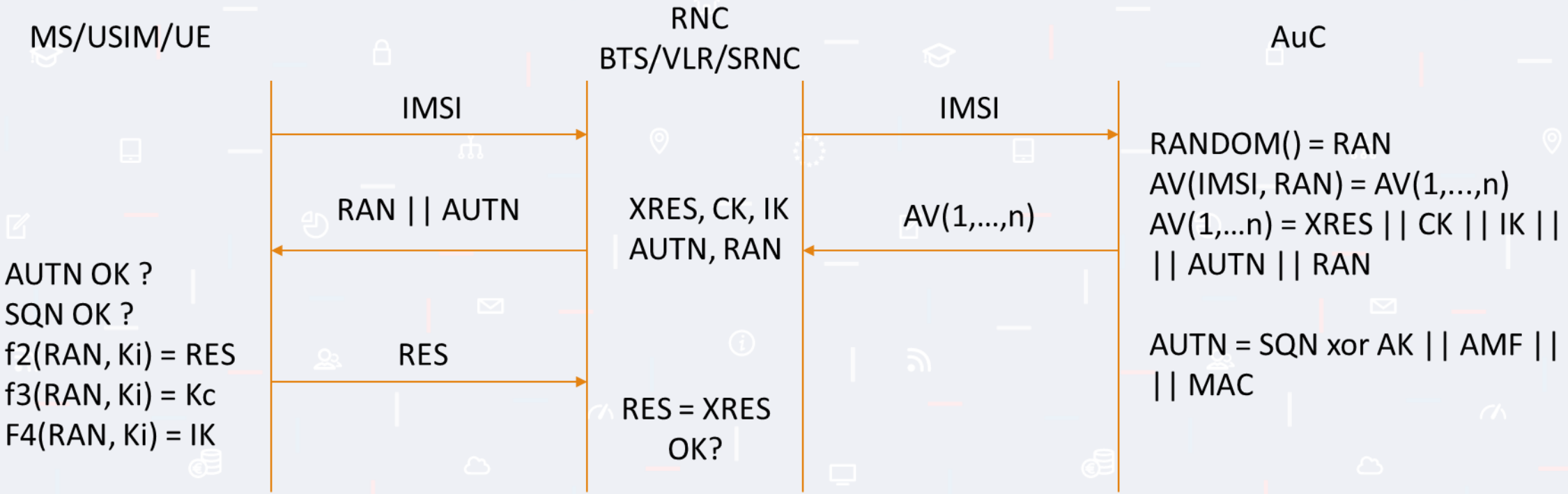
+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE

Fukncia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	…	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na USIM – zdieľaný s AuC	Žiadny	USIM, AuC		128

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

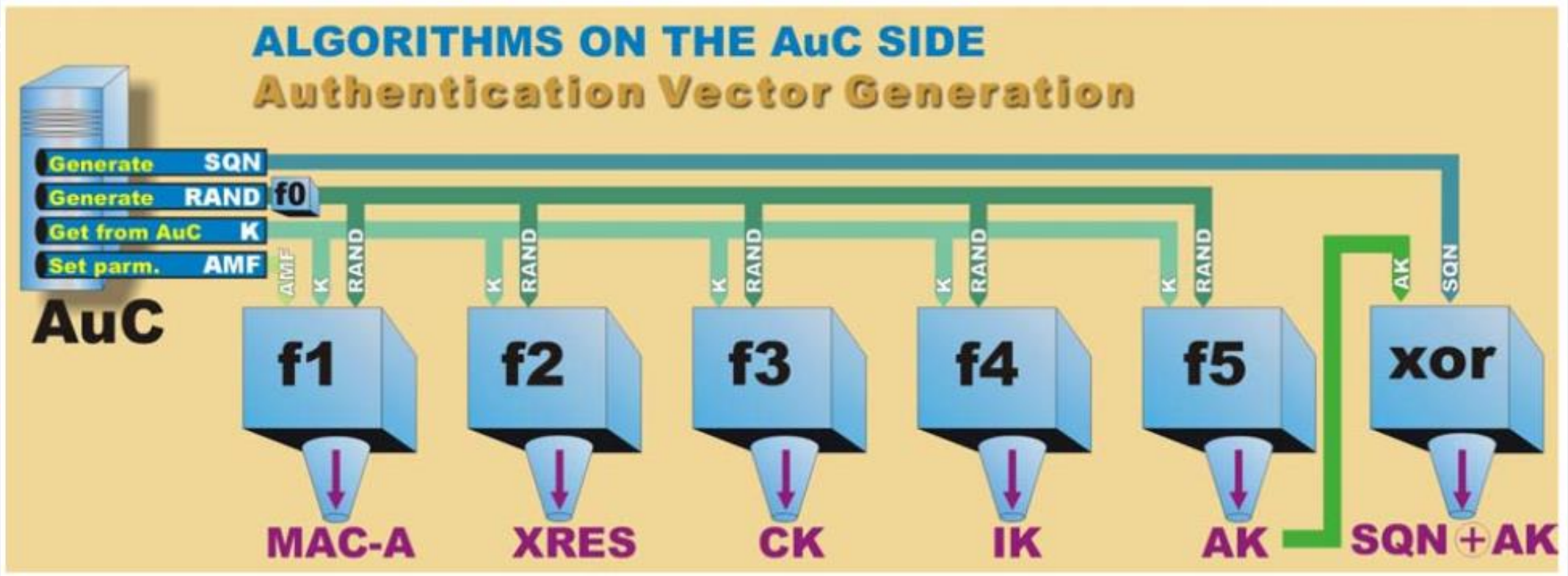
Algoritmy

- GSM:
  - ENC: A5/1 & A5/2
  - COMP128: A3 – 32 bit, A8 – 64 bit
    - Utajované
- 3G:
  - ENC: KASUMI (GEA0, GEA1) -> RNC CHOOSE ENC. -> MS
  - f9: Milenage
- 4G:
  - ENC: Snow 3G || AES 128b.

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

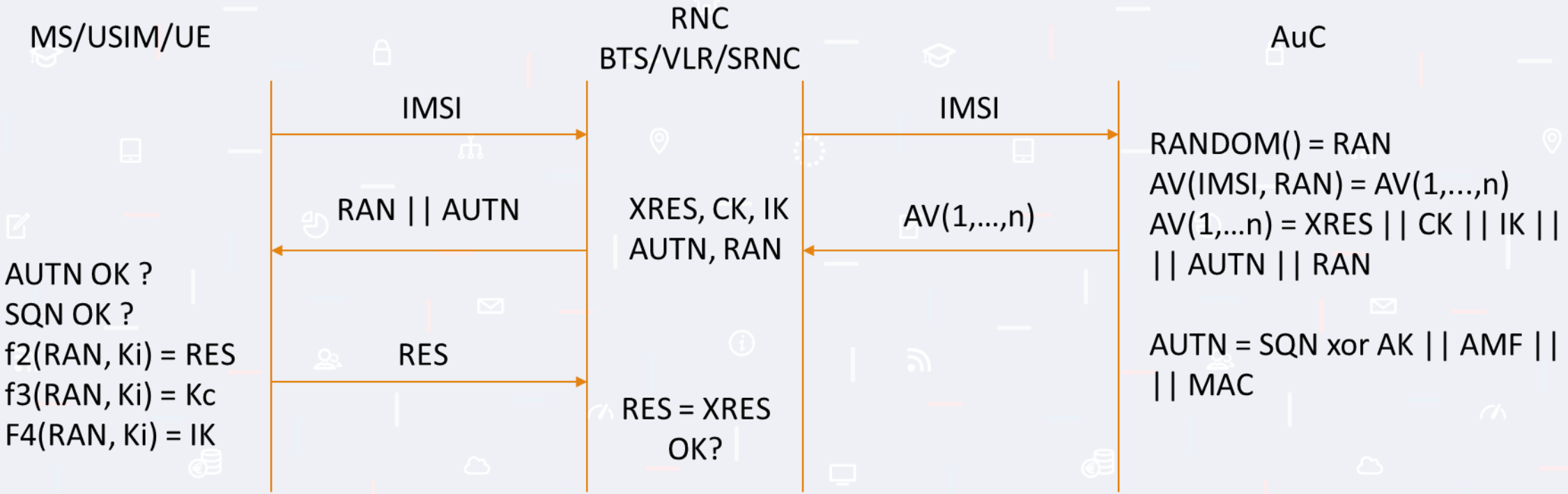
3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk

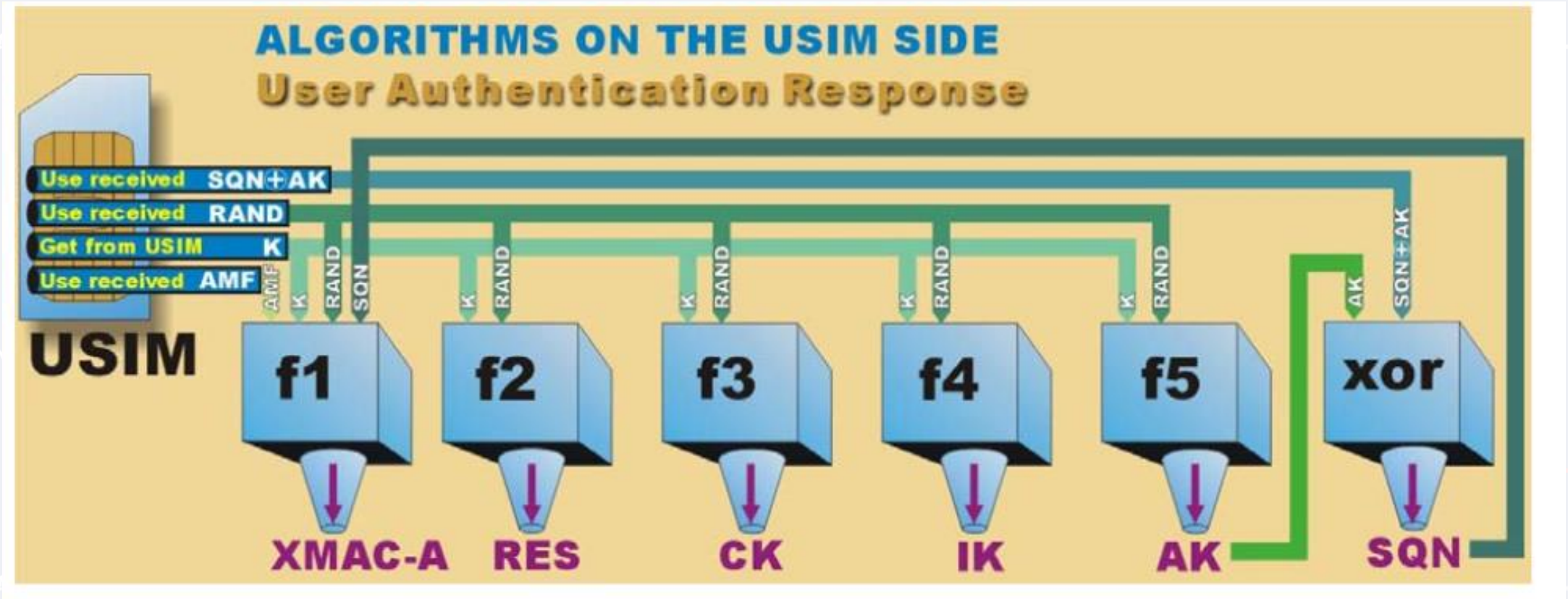
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

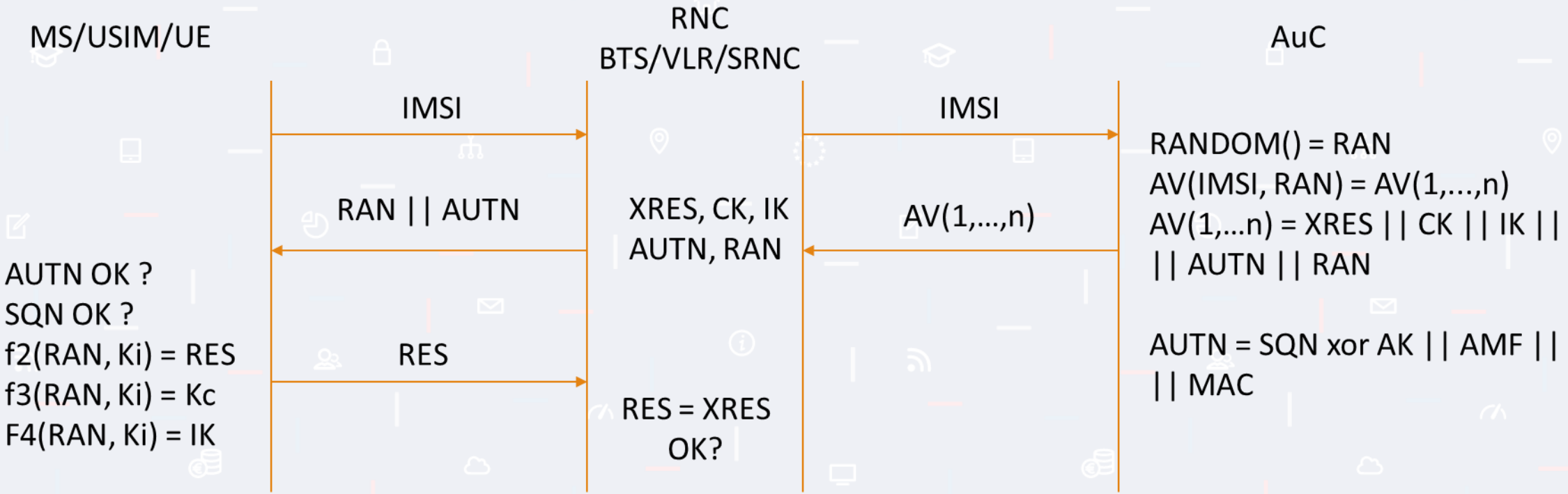
3G a LTE



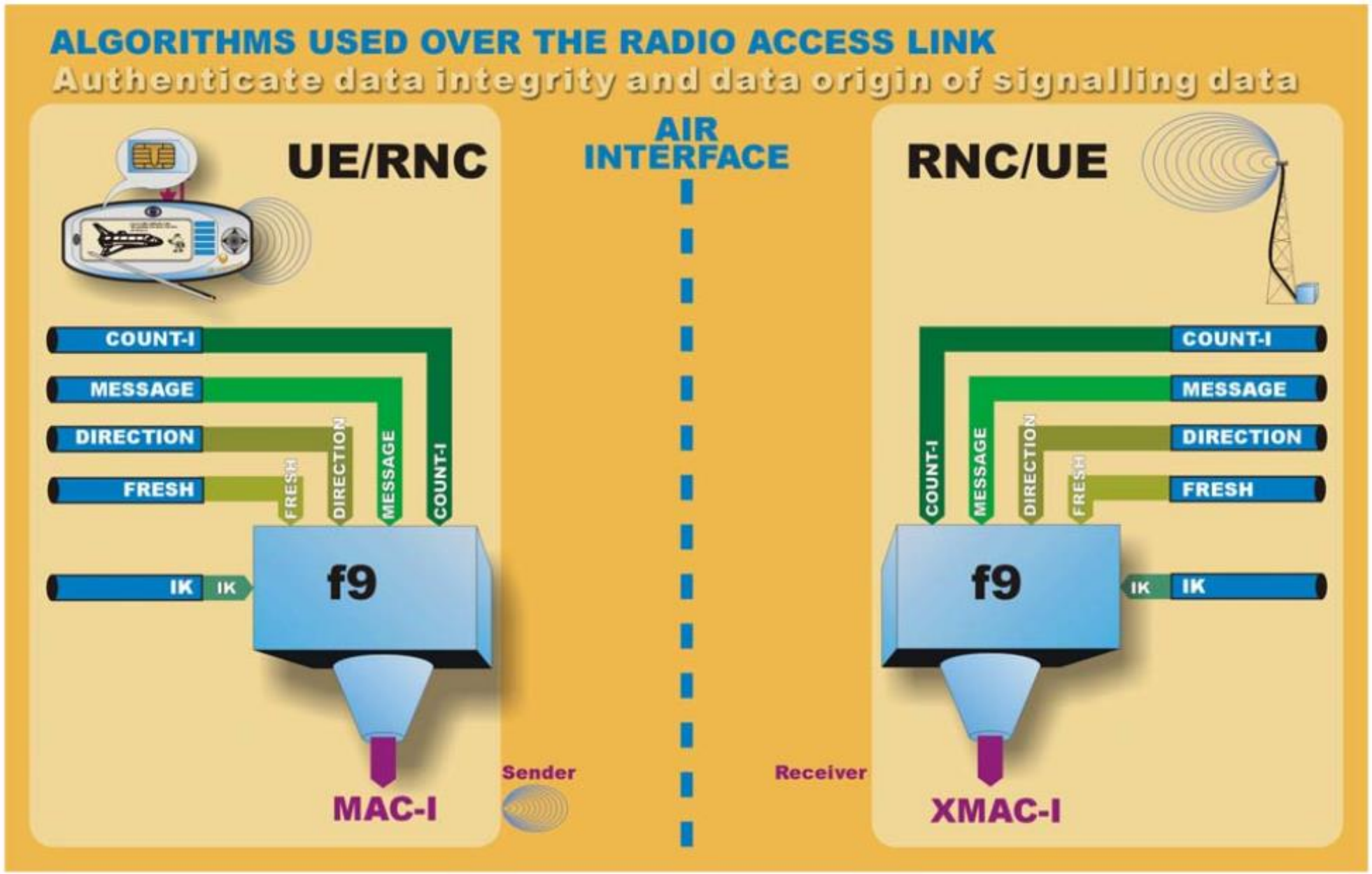
+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE

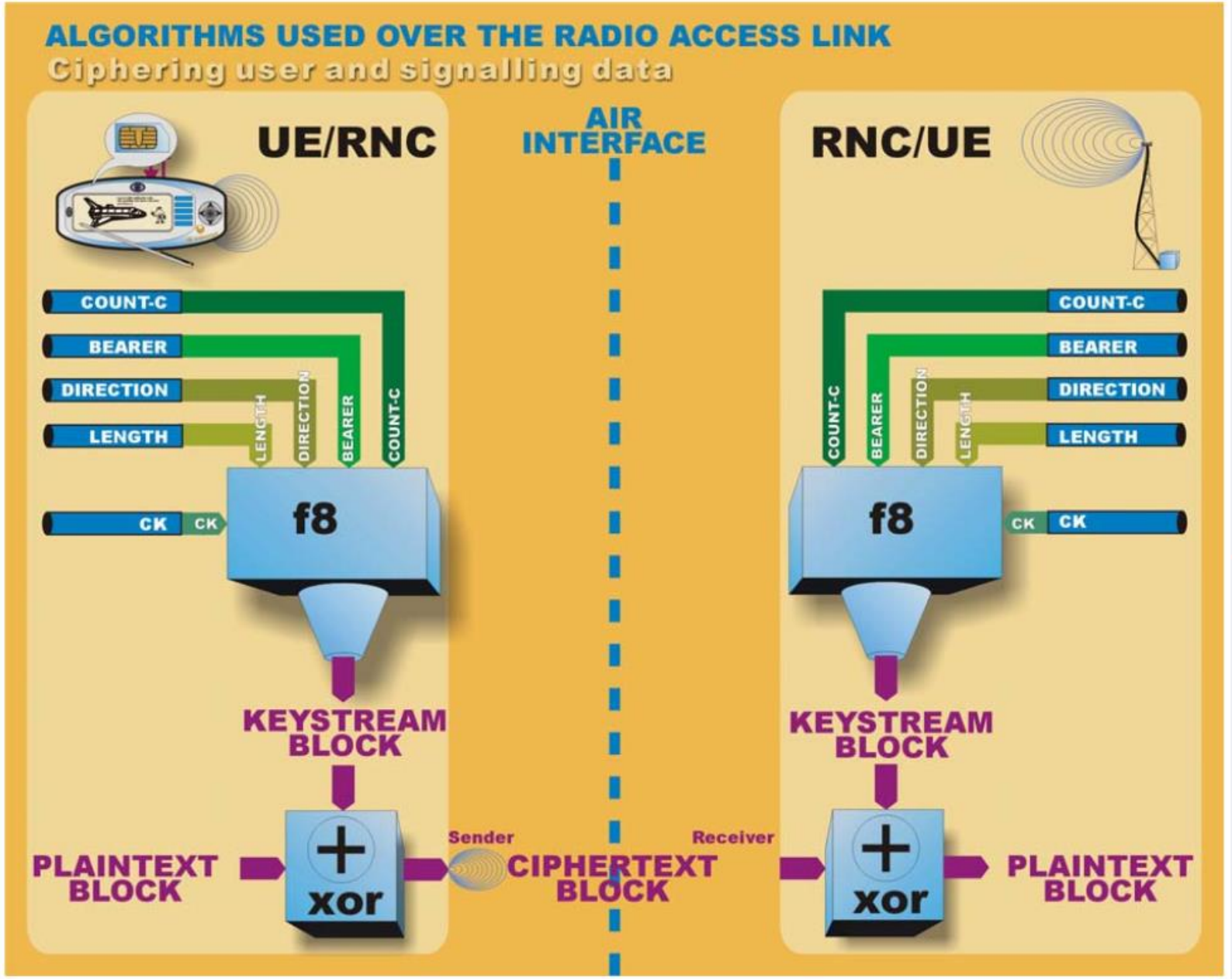


+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk


ALGORITHMS USED OVER THE RADIO ACCESS LINK
Ciphering user and signalling data
UE/RNC
AIR INTERFACE
RNC/UE
COUNT-C
BEARER
DIRECTION
LENGTH
CK
f8
KEYSTREAM BLOCK
PLAINTEXT BLOCK
xor
Sender
CIPHERTEXT BLOCK
Receiver

Lamanie A5/1
Rainbow tables
Time memory data tradeoff

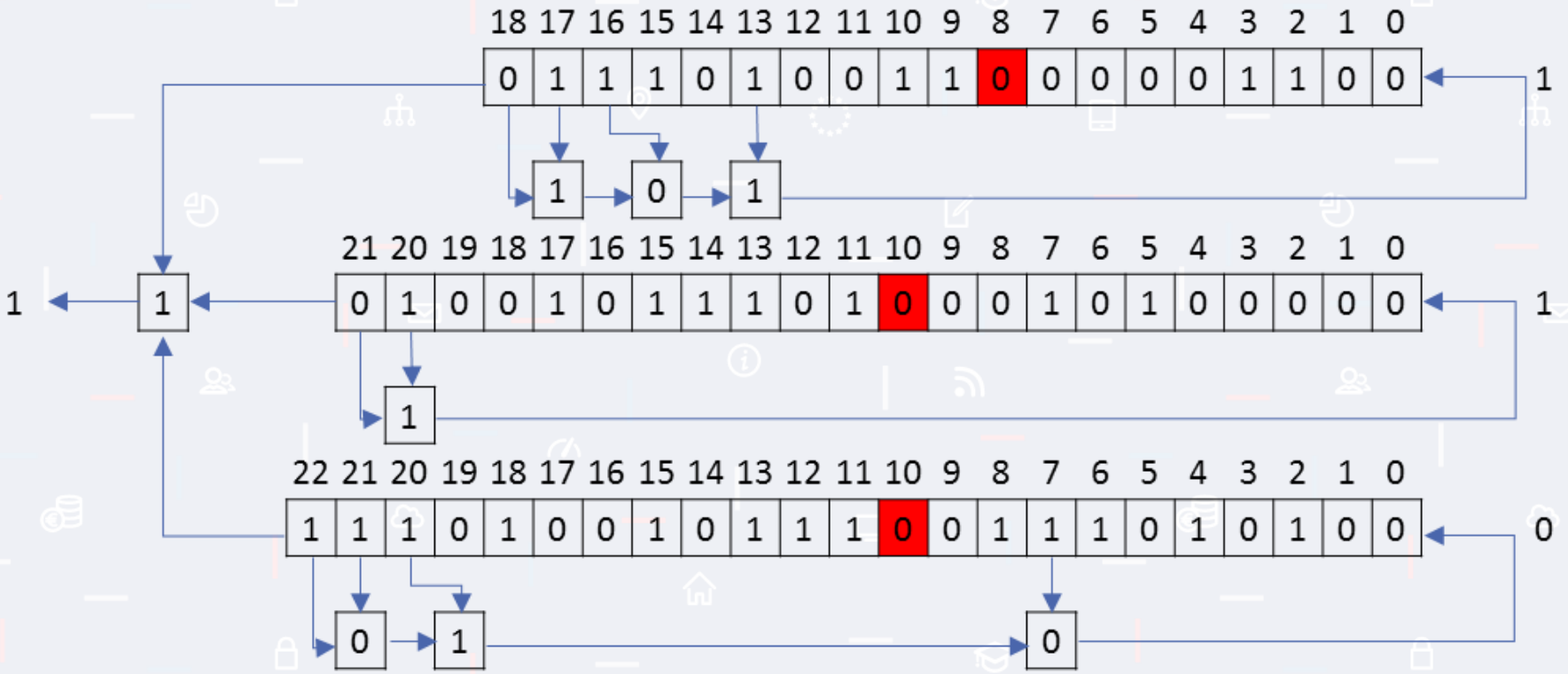
A5/1

- Prúdové šifry
- Kryptoanalýza v reálnom čase
- BTS simulácia
  - Náročná implementácia
  - bb.osmocom.org
  - 5x Motorola C155 15$ || bladeRF x40 420$
- RTL-SDR
- Armáda (agáta)

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1

- 2^{61} - počet možných stavov
- Chris Paget a Karsten Nohl
  - 2 TB predpočítaných dát
  - Zdielané známou P2P sieťou
  - Pár sekúnd = prelomená A5/1
- Time-memory-data tradeoff
  - S určitou pravdepodobnosťou
  - Rainbow table
- NOP správy
- Detekovanie kľúča

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1 Time-Memory-data tradeoff

64b

000…1	→	Koncový bod
000…2	→	Koncový bod
000…3	→	Koncový bod
.		
.		
.		
fff…f	→	Koncový bod

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1 Time-Memory-data tradeoff

2^{64}

64b

000…1 → Koncový bod

000…2 → Koncový bod

000…3 → Koncový bod

.

.

.

fff…f → Koncový bod

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1 Time-Memory-data tradeoff

64b

000…1 → A5/1 → A5/1 … → A5/1 → Koncový bod

000…2 → A5/1 → A5/1 … → A5/1 → Koncový bod

000…3 → A5/1 → A5/1 … → A5/1 → Koncový bod

.

.

.

fff…f → A5/1 → A5/1 … → A5/1 → Koncový bod

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1 Time-Memory-data tradeoff

64b

000…1 → A5/1 → A5/1 … → A5/1 → …0000

000…2 → A5/1 → A5/1 … → A5/1 → …0000

000…3 → A5/1 → A5/1 … → A5/1 → …0000

.

.

.

fff…f → A5/1 → A5/1 … → A5/1 → …0000

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1 Time-Memory-data tradeoff

64b

000…1 → A5/1 → A5/1 … → A5/1 → …0000

000…2 → A5/1 → A5/1 … → A5/1 → …0000

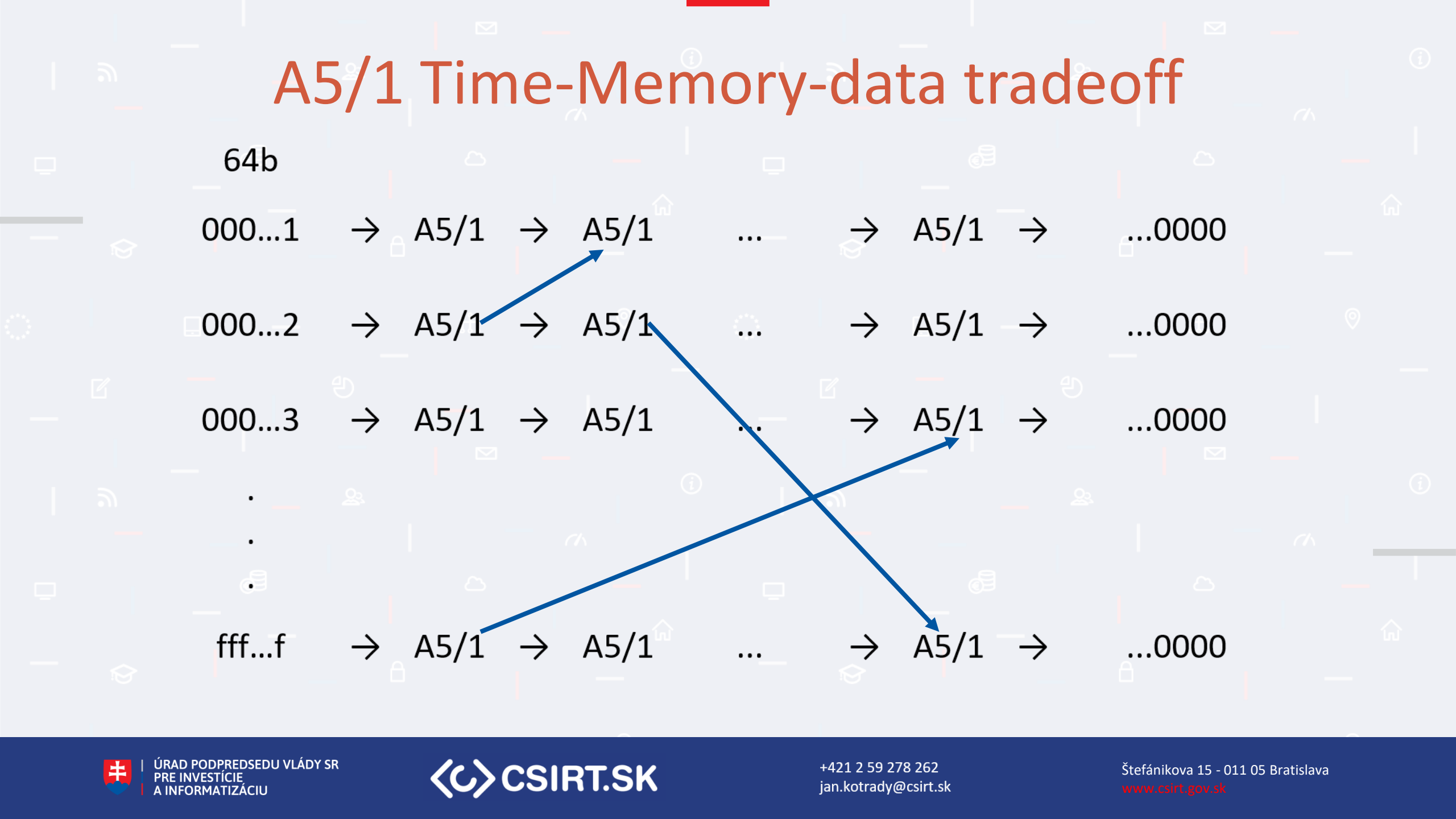
000…3 → A5/1 → A5/1 … → A5/1 → …0000

.

.

.

fff…f → A5/1 → A5/1 … → A5/1 → …0000



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1 Time-Memory-data tradeoff

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

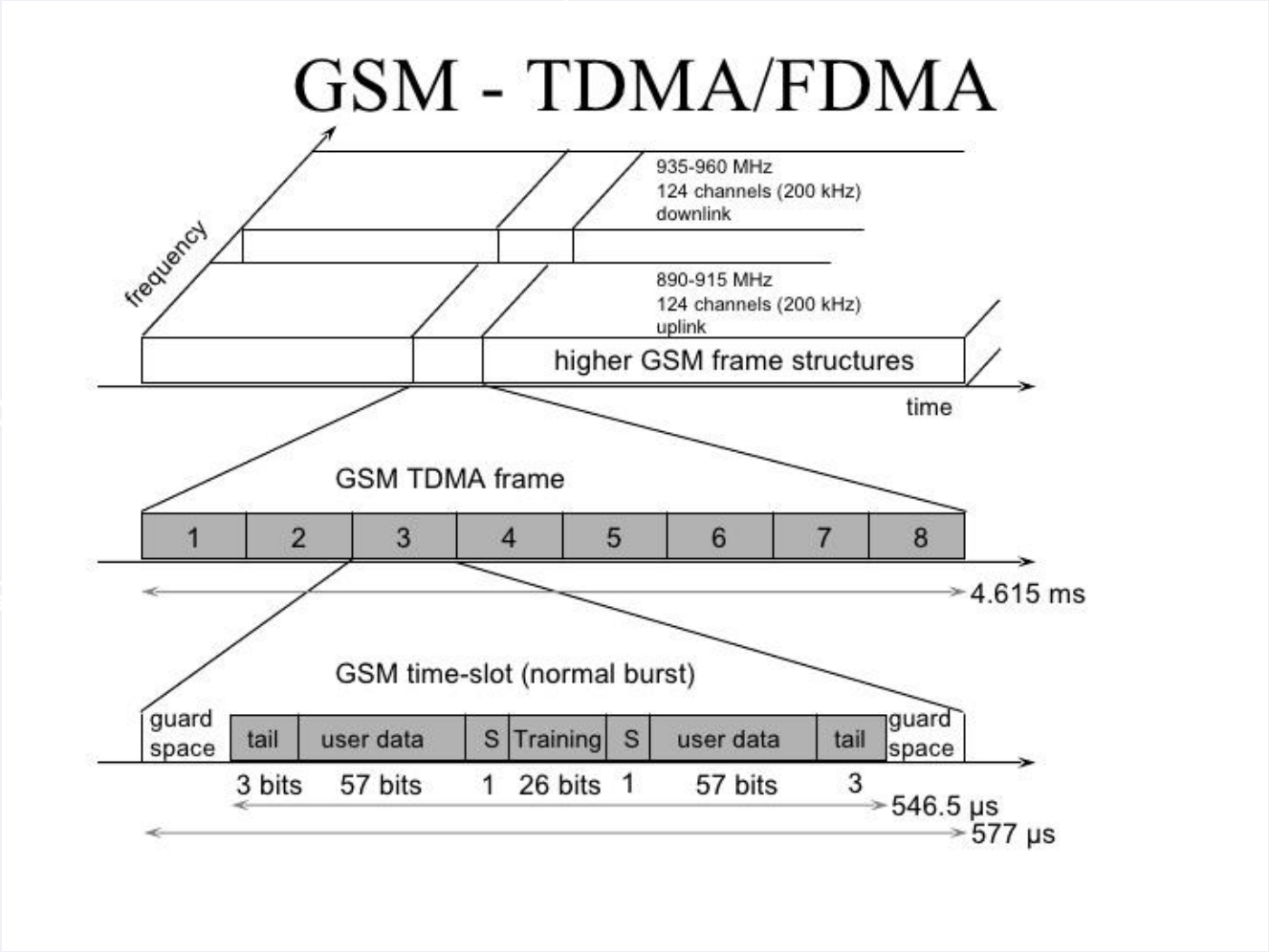
A5/1

- 2^{61} - počet možných stavov
- Naivná tabuľka: 296 EB (exabajt)
- Zredukovanie vnútorných stavov o 3 bity (efektívny počet bitov): 37 EB
- GSM Frame 4x po 114 bitov – potrebujeme len 64 => 204 rôznych posunov 37/204
- Zavedenie 4096 blokov -> 37/204/4096 = 44 TB
- Zavedenie 8 farieb = 5,5 TB
- Zredukovanie výšky tabuľky na 2^{34} a použijeme hash
- Zakódovanie endpointu = 1.8T

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Frame, burst



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Správy nop

- Fixný text
- Nemám ti čo povedať, ale niečo hovorím ☺

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1

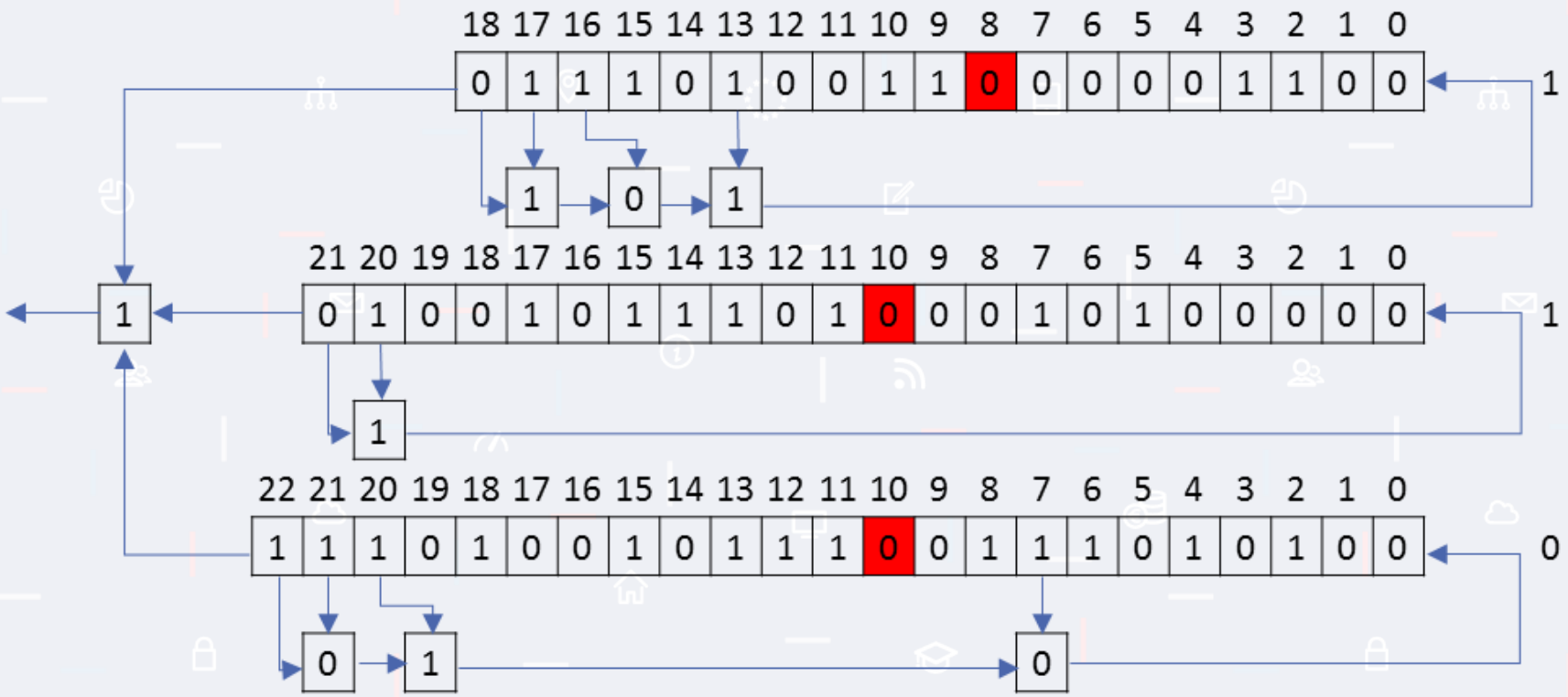
NOP

⊕

1011001011100

=

1101110001101



A5/1

NOP

⊕

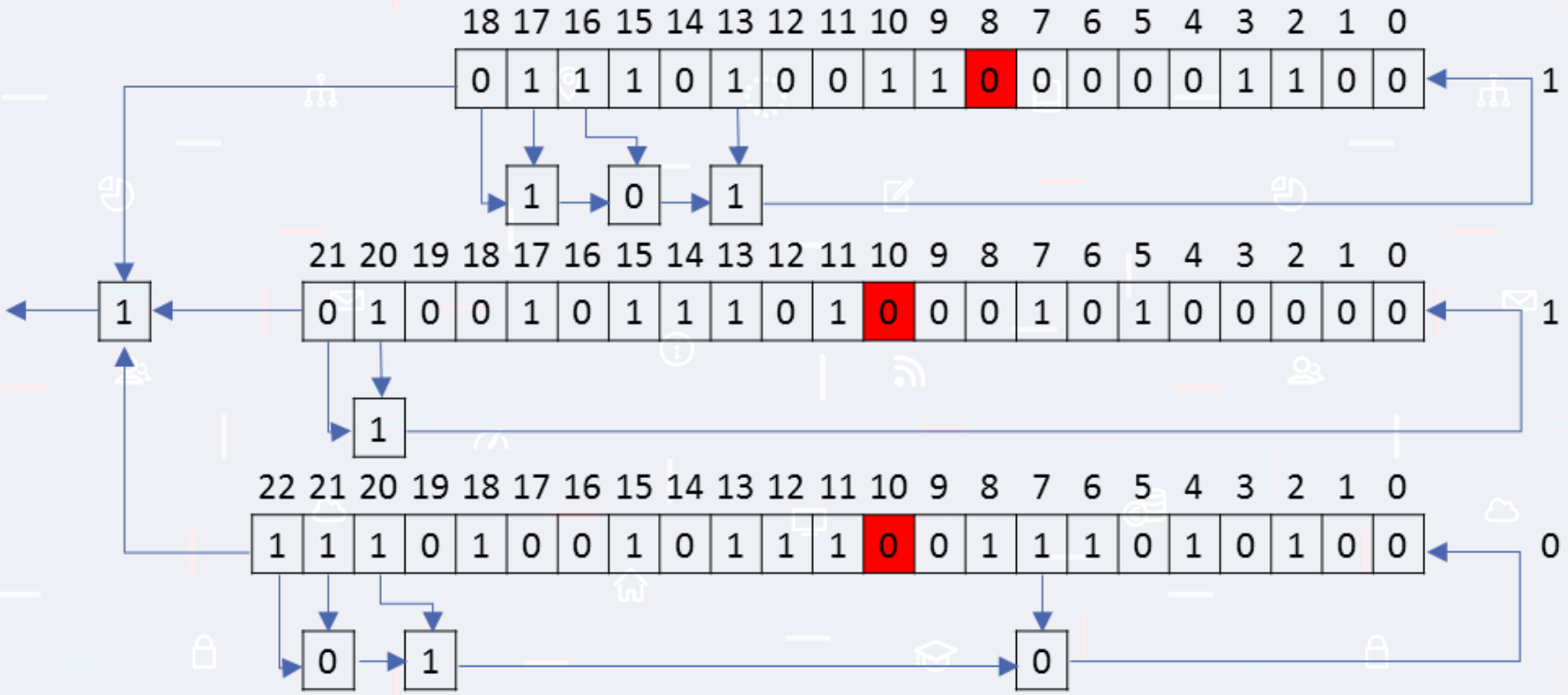
1011001011100

=

1101110001101

⊕

NOP



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1

NOP

⊕

1011001011100

=

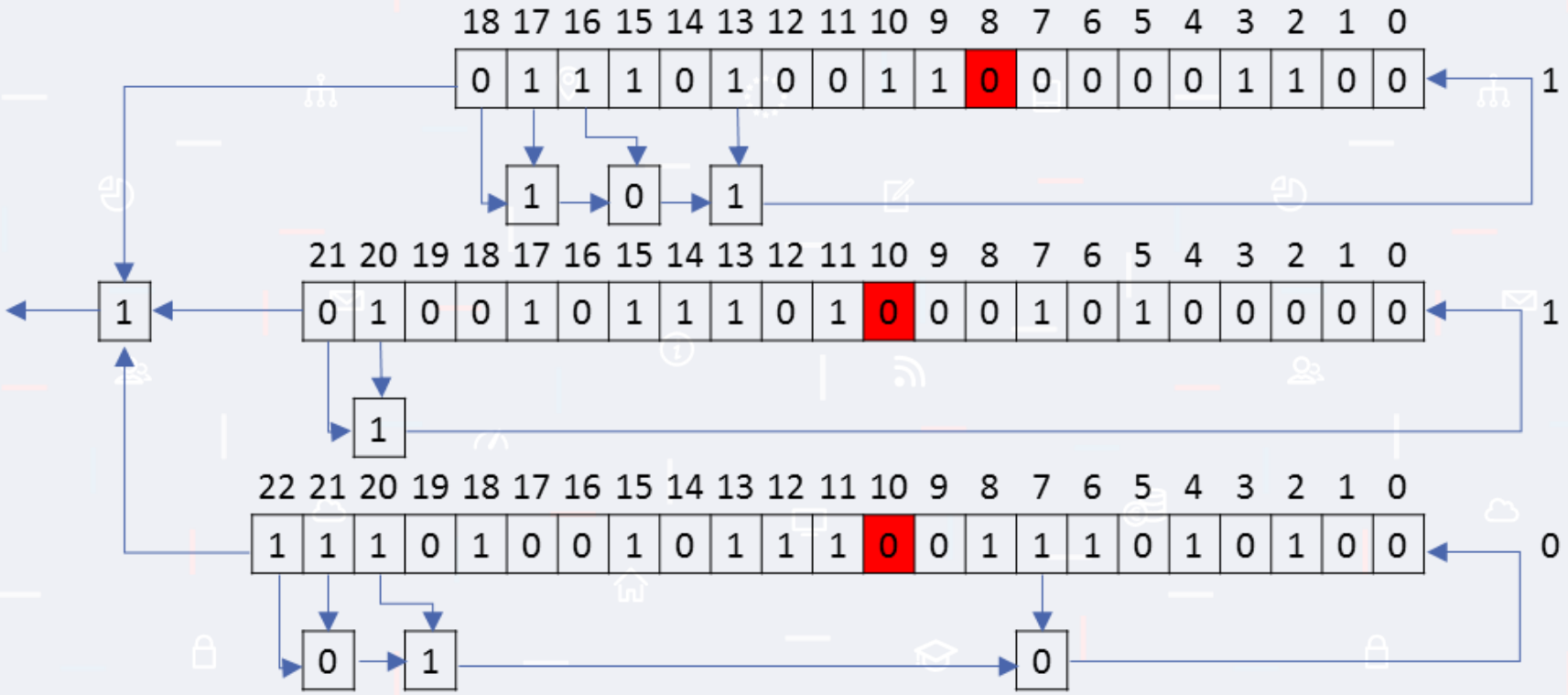
1101110001101

⊕

NOP

=

1011001011100



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

A5/1

XOR operácie			
1	⊕	1	0
1	⊕	0	1
0	⊕	1	1
0	⊕	0	0

NOP

⊕

1011001011100

=

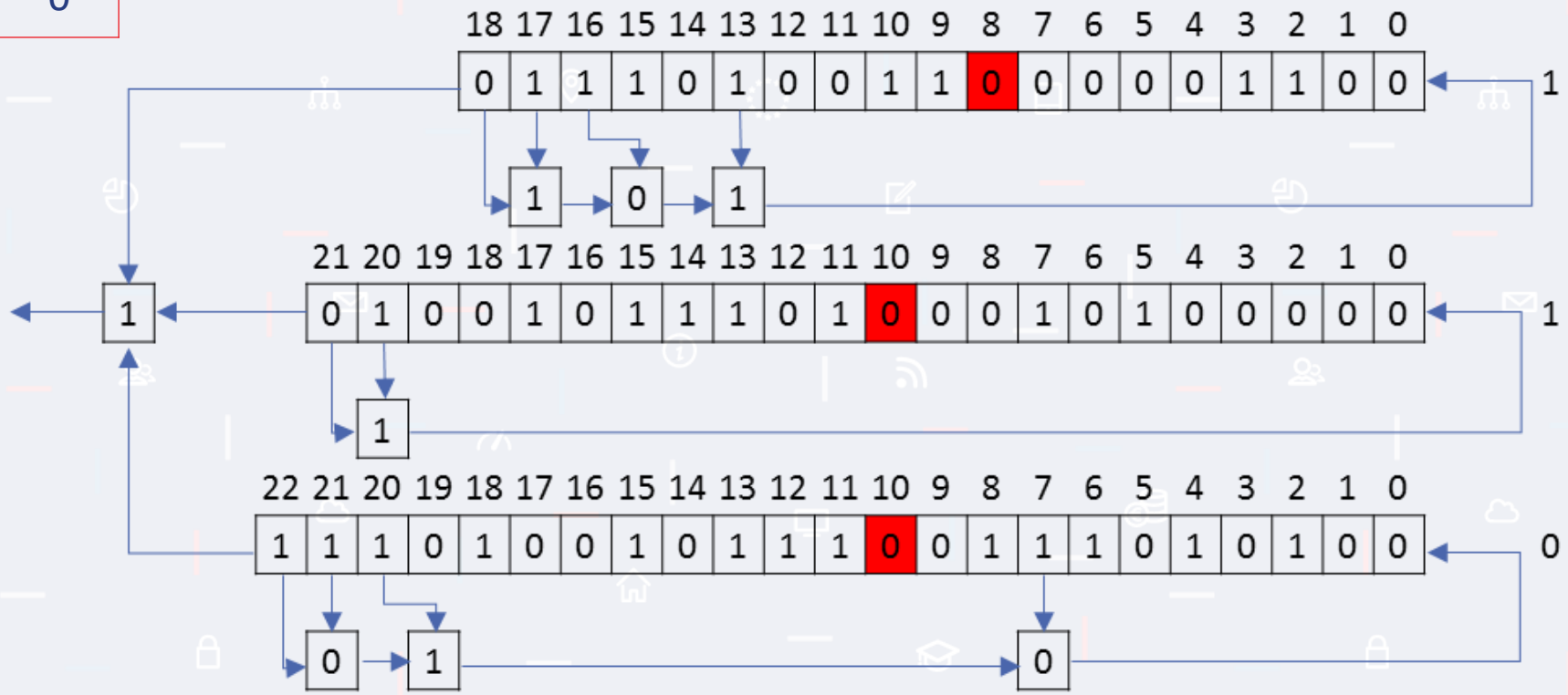
1101110001101

⊕

NOP

=

1011001011100



+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Frame

- Každý frame má svoje číslo
- Číslo je verejné známe
- Každý frame ma niekoľko burstvo
- Každý burst je šifrovaný individuálne

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

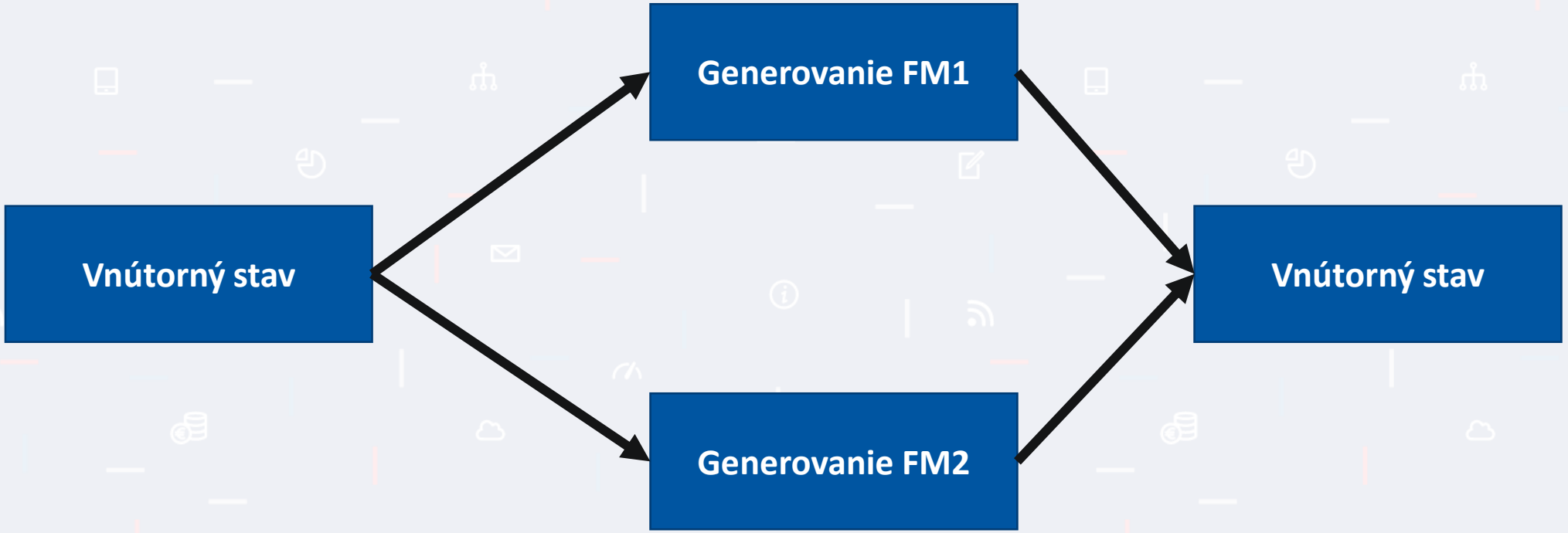
Frame update

- Každý frame má svoje číslo
- Číslo je verejné známe
- Každý frame ma niekoľko burstvo
- Každý burst je šifrovaný individuálne
- NOP ma nahodný padding
  - rainbow tabuľky na základe frame number

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Dešifrovanie na základe Frame number



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ďalšie možnosti

- Snoopsnitch
- SS7 protokol
- IMSI catcher
- Falošná BTS
- Falošný operátor
- ...

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Zdroje

- https://brage.bibsys.no/xmlui/bitstream/handle/11250/137418/master_ikt_2001_dohmen.pdf?sequence=1
- http://www.netlab.tkk.fi/opetus/s38153/k2003/Lectures/g42UMTS_security.pdf

Pre 4G (LTE):

- http://www.ijritcc.org/download/1430372773.pdf

Klonovanie (U)SIM kariet:

- https://www.blackhat.com/docs/us-15/materials/us-15-Yu-Cloning-3G-4G-SIM-Cards-With-A-PC-And-An-Oscilloscope-Lessons-Learned-In-Physical-Security.pdf

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ďakujem
za pozornosť